

УДК 004.056:378.147

**Ануар Әлімжан Бахытжанұлы**

магистрант

кафедра «Информационная безопасность»

Евразийский национальный университет им. Л.Н. Гумилева

(г. Астана, Казахстан)

**Сексенбаева Айша Курманбековна**

к.ф.-м.н., доцент

кафедра «Информационная безопасность»

Евразийский национальный университет им. Л.Н. Гумилева

(г. Астана, Казахстан)

## **СРАВНИТЕЛЬНЫЙ АНАЛИЗ СТАНДАРТОВ И МЕТОДИК ОБУЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ: NICE FRAMEWORK, ECSF И ПРАКТИКО- ОРИЕНТИРОВАННЫЕ ТЕХНОЛОГИИ**

**Аннотация:** Сравниваются две ведущие рамки компетенций по кибербезопасности: американская NICE Framework (NIST SP 800-181) и европейская European Cybersecurity Skills Framework (ECSF), разработанная ENISA. Отдельно разобраны современные практико-ориентированные форматы обучения, то есть киберполигоны, изолированные учебные среды («песочницы»), CTF-соревнования, геймификация и адаптивное обучение на базе искусственного интеллекта. Актуальность подкрепляется казахстанской статистикой: за I квартал 2025 г. инцидентов информационной безопасности в стране зарегистрировано более чем вдвое больше, чем за тот же квартал 2024 г. Стандарты сопоставлялись по единому списку критериев; помимо них рассмотрены пять международных образовательных платформ и научные публикации 2019–2026 гг. NICE Framework детальнее описывает задачи, знания и навыки. С ECSF же проще проектировать образовательную программу: профилей ролей в ней всего двенадцать, и рамка увязана с e-CF и EQF. Авторы предлагают матрицу соответствия «профиль роли — ведущий метод обучения» и смешанную модель подготовки, где адаптивная теория, практика в изолированных средах и игровой контроль работают в связке. Для вузов Республики Казахстан сформулированы рекомендации по обновлению образовательных программ.

**Ключевые слова:** кибербезопасность, NICE Framework, ECSF, рамка компетенций, киберполигон, CTF, геймификация, адаптивное обучение, человеческий фактор, Казахстан.

### **Введение**

Устойчивое цифровое развитие государства сегодня трудно представить без кибербезопасности. Сложность в том, что атак становится больше и они усложняются быстрее, чем успевают готовить специалистов. ОЭСР, изучив ситуацию во Франции, Германии и Польше, констатирует хроническую нехватку квалифицированных кадров в этой сфере и расхождение между тем, чему учат образовательные программы, и тем, что нужно работодателям [1].

В Казахстане проблема ощущается особенно остро. Ranking.kz, обобщив данные KZ-CERT, приводит такие цифры: в январе–марте 2025 г. зарегистрировано 29 982

инцидента информационной безопасности, а за январь–март 2024 г. их было 14 868, то есть прирост составил 101,7 % [2]. Как инциденты распределяются по типам, видно из таблицы 1.

**Таблица 1 – Инциденты информационной безопасности в Республике Казахстан, январь–март, ед. (составлено авторами по [2])**

| Тип инцидента                                       | 2024 г. | 2025 г. | Прирост, % | Доля в 2025 г., % |
|-----------------------------------------------------|---------|---------|------------|-------------------|
| Ботнеты                                             | 1 748   | 17 606  | +907,2     | 58,7              |
| Вирусы, сетевые черви, трояны                       | 9 586   | 7 870   | –17,9      | 26,2              |
| Фишинг                                              | 1 439   | 1 975   | +37,2      | 6,6               |
| Отсутствие доступа к интернет-ресурсу               | 216     | 112     | –48,1      | 0,4               |
| DoS/DDoS-атаки                                      | 30      | 23      | –23,3      | 0,1               |
| Несанкционированный доступ и модификация содержания | 13      | 9       | –30,8      | 0,0               |
| Прочие инциденты                                    | 1 836   | 2 387   | +30,0      | 8,0               |
| Всего                                               | 14 868  | 29 982  | +101,7     | 100,0             |

Сильнее всего выросли ботнет-активность и фишинг, а успех этих угроз во многом зависит от того, как действуют пользователи и администраторы. Среди стран СНГ на Казахстан приходится около 8 % успешных атак; доля DDoS-атак в целом по СНГ составляет 18 %, что более чем вдвое выше среднемировых 8 % [3]. Авторы глобальных обзоров отмечают, что злоумышленники всё чаще автоматизируют атаки и подключают инструменты искусственного интеллекта, из-за чего учебное содержание приходится постоянно обновлять [4; 5].

Самым уязвимым звеном защиты по-прежнему остаётся человеческий фактор. Социальная инженерия эксплуатирует доверие, любопытство и готовность помочь [6]. Как выяснили Pahlila и соавт., соблюдение сотрудниками политик ИБ определяется не одними знаниями: свою роль играют установки, привычки и намерение следовать правилам [7]. Значит, обучающимся нужно прививать устойчивые модели поведения, а для этого требуются практико-ориентированные методы. На национальном уровне задачи развития отрасли закреплены в Концепции цифровой трансформации, развития отрасли ИКТ и кибербезопасности на 2023–2029 гг. [8].

Разрабатывая образовательные программы, вузы ориентируются на международные стандарты компетенций, в первую очередь на NICE (США) и ECSF (ЕС). По наблюдениям авторов, учебная база при этом отстаёт от того, как меняются киберугрозы: лабораторные практикумы и инструменты быстро устаревают. Работ, в которых эти рамки сопоставлялись бы между собой и увязывались с актуальными педагогическими методиками, в отечественной литературе пока немного.

**Цель исследования** заключается в обосновании модели практико-ориентированной подготовки специалистов по кибербезопасности для вузов Республики Казахстан. Модель строится на сравнении рамок компетенций NICE и ECSF и современных методов обучения.

**Задачи исследования:**

- 1) сопоставить NICE Framework и ECSF по общему набору критериев;
- 2) изучить ведущие международные образовательные платформы;
- 3) обобщить данные об эффективности практико-ориентированных методов обучения;
- 4) соотнести профили ролей с методами обучения и предложить гибридную модель подготовки.

### **Материалы и методы**

Работа имеет аналитический характер и опирается на три метода, которые дополняют друг друга.

**1. Сравнительный документальный анализ стандартов.** В качестве объектов анализа взяты публикация NIST SP 800-181 Rev. 1 [9], действующие компоненты NICE Framework [10], а также профили ролей и руководство пользователя ECSF [11; 12]. Документы сравнивались по следующим критериям: разработчик и статус документа, его структура и единица описания, количество ролей, степень детализации, связь с квалификационными системами, наличие инструментов для разработки учебных программ и ограничения, которые возникают при применении в Казахстане.

**2. Сравнительный анализ образовательных платформ.** Пять международных платформ (Cybrary, Coursera, Udemy, Hack The Box, TryHackMe) сравнивались по основной специализации, формату контента, модели доступа и наличию практической среды. Информация взята из открытых описаний самих платформ.

**3. Обзор научных публикаций.** В выборку вошли работы 2019–2026 гг. из Scopus, IEEE Xplore, SpringerLink и ScienceDirect, найденные по запросам «cybersecurity education», «gamification», «cyber range», «security awareness», а также классические труды по теории обучения. Публикации без эмпирических данных или теоретического обоснования методов в анализ не включались.

По итогам трёх этапов составлена сводная матрица «профиль роли — метод обучения», и уже на её основе предложена гибридная модель подготовки.

### **Теоретические основы и обзор литературы**

Теоретическую основу практико-ориентированного обучения задаёт модель экспериментального обучения Д. Колба. По Колбу, прочное знание складывается в цикле «конкретный опыт — рефлексия — концептуализация — активное экспериментирование» [13]. Из теории когнитивной нагрузки Дж. Свеллера следует, что сложность заданий нужно дозировать, а на первых этапах полезно опираться на пошаговые примеры [14]. Андрагогический подход М. Ноулза исходит из того, что взрослые лучше усваивают материал, который напрямую связан с их профессиональными задачами [15]. Мотивацию объясняет теория самодетерминации Э. Деси и Р. Райана: внутренняя мотивация сохраняется, когда удовлетворены потребности в компетентности, автономии и причастности [16].

По данным систематического обзора Hamari и соавт., геймификация в целом даёт положительный эффект, однако он зависит от контекста и от особенностей пользователей [17]. Для сферы информационной безопасности Pahlavanpour и Gao в систематическом картировании показали, что исследований геймифицированных программ повышения осведомлённости становится больше, но строгих оценок их долгосрочного эффекта по-прежнему не хватает [18].

Эмпирические работы эту неоднозначность подтверждают. В эксперименте Weijnsfeld и Sarmah у студентов, изучавших стеганографию через сюжетную игру,

вовлечённость была значимо выше, однако по результатам теста знаний статистически значимой разницы с традиционным форматом не обнаружилось [19]. Mpanza, Gundu и Fatcher сформулировали практические рекомендации по применению геймификации против социальной инженерии [20]. Veneruso и соавт. показали, как виртуальную реальность можно использовать для обучения безопасному поведению [21]. По данным Fertig и соавт., e-learning-платформы помогают повысить осведомлённость в вопросах информационной безопасности [22], а Hijji и Alam разработали рамку обучения для сотрудников, работающих удалённо [23].

О разрыве между академической подготовкой и запросами практики говорят давно: ещё в 2000-х гг. исследователи предлагали сместить акцент программ на практические навыки и разрабатывать учебные планы вместе с отраслью [24; 25].

Из обзора следуют три вывода. Во-первых, практико-ориентированные и игровые методы стабильно повышают вовлечённость. Во-вторых, их влияние на объём знаний неоднозначно и определяется тем, как выстроено обучение. В-третьих, ни один метод сам по себе не охватывает всех компетенций, поэтому методы нужно обоснованно сочетать и привязывать к профессиональным ролям.

## Результаты

### 1. Сравнение рамок компетенций NICE и ECSF

Итоги сравнения представлены в таблице 2.

**Таблица 2 – Сравнение NICE Framework и ECSF (составлено авторами по [9–12])**

| Критерий               | NICE Framework (США)                                                                                                 | ECSF (Европейский союз)                                                           |
|------------------------|----------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| Разработчик, год       | NIST; SP 800-181 (2017), Rev. 1 (2020); компоненты обновляются регулярно (v1.0.0 — 2024 г., v2.2.0 — апрель 2026 г.) | ENISA; сентябрь 2022 г.                                                           |
| Структура              | 7 категорий рабочих ролей → рабочие роли → утверждения о задачах, знаниях и навыках (TKS); области компетенций       | 12 профилей ролей по единому шаблону                                              |
| Единица описания       | Отдельное утверждение TKS (модульный «конструктор»)                                                                  | Профиль роли: миссия, результаты, задачи, ключевые навыки и знания, е-компетенции |
| Объём (v1.0.0)         | 52 рабочие роли, 11 областей компетенций, около 2 280 утверждений TKS                                                | 12 профилей                                                                       |
| Связь с квалификациями | Прямой связи с уровнями квалификаций нет                                                                             | Связь с е-CF (EN 16234-1, уровни e-1...e-5) и через неё с EQF                     |
| Инструменты для вузов  | Программа центров компетенций (CAE), каталоги курсов NICCS                                                           | Проекты SPARTA (конструктор учебных программ) и CONCORDIA (каталог курсов)        |

| Критерий           | NICE Framework (США)                                                         | ECSF (Европейский союз)                                                                         |
|--------------------|------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|
| Сильные стороны    | Высокая детализация, точная привязка заданий к задачам                       | Компактность, понятность для работодателей и вузов, совместимость с европейскими квалификациями |
| Ограничения для РК | Избыточна для бакалавриата; часть ролей связана со спецификой госсектора США | Меньшая детализация; нет готовых измеримых индикаторов для оценки                               |

Получается, что рамки дополняют друг друга. ECSF удобно применять на уровне образовательной программы, чтобы задать траектории выпускника, а NICE лучше подходит для уровня дисциплин и отдельных заданий, где проверяемые навыки нужно сформулировать точно.

## 2. Сравнение образовательных платформ

**Таблица 3 – Сравнение международных платформ обучения кибербезопасности**

| Платформа    | Специализация                       | Формат контента                | Модель доступа                   | Практическая среда            |
|--------------|-------------------------------------|--------------------------------|----------------------------------|-------------------------------|
| Cybrary      | Подготовка к сертификации           | Видеолекции, лабораторные      | Подписка (есть бесплатная часть) | Виртуальные лаборатории       |
| Coursera     | Академические курсы вузов           | Курсы, специализации           | Оплата курса или подписка        | Проекты в браузере            |
| Udemy        | Прикладные навыки от практиков      | Видеоуроки, тесты              | Разовая покупка курса            | Зависит от автора             |
| Hack The Box | Наступательная безопасность, CTF    | Уязвимые машины, киберполигоны | Freemium / подписка              | Реальные цели через VPN       |
| TryHackMe    | Сценарное обучение (learning paths) | Интерактивные «комнаты»        | Freemium / подписка              | Встроенные виртуальные машины |

Платформы с игровыми механиками (Hack The Box, TryHackMe) сразу дают обратную связь и добавляют элемент соревнования, но управленческие и правовые компетенции почти не затрагивают. Академические платформы (Coursera, Udemy) хорошо закладывают теорию, а практики в них немного. Весь спектр ролей ECSF не охватывает ни одна из платформ.

## 3. Матрица методов обучения

**Таблица 4 – Сравнительная характеристика практико-ориентированных методов**

| Метод                      | Ключевой механизм                         | Основное преимущество                                   | Ограничение                                        |
|----------------------------|-------------------------------------------|---------------------------------------------------------|----------------------------------------------------|
| Геймификация               | Баллы, уровни, рейтинги, сюжет            | Рост вовлечённости и мотивации [17–19]                  | Эффект на знания неоднозначен; риск упрощения [19] |
| Песочница (sandbox)        | Изолированная среда выполнения            | Безопасный анализ вредоносного ПО и ошибок              | Требования к инфраструктуре                        |
| Киберполигон (cyber range) | Моделирование атак на инфраструктуру      | Навыки реагирования и командной работы                  | Сложность и стоимость сценариев                    |
| CTF-соревнования           | Задачи с «флагом», ограничение по времени | Объективная оценка навыков в стрессовых условиях        | Смещение в сторону технических ролей               |
| Адаптивное обучение (ИИ)   | Подстройка сложности под обучающегося     | Индивидуальный темп, контроль когнитивной нагрузки [14] | Нужны данные и качественный контент                |

Сопоставление профилей ECSF (вместе с соответствующими категориями NICE) и методов обучения позволило построить матрицу соответствия (таблица 5). Она и составляет основной авторский результат исследования.

**Таблица 5 – Матрица соответствия «профиль роли — ведущий метод обучения» (разработано авторами)**

| Профиль ECSF                                    | Категория NICE                                       | Ведущий метод                               | Форма контроля                |
|-------------------------------------------------|------------------------------------------------------|---------------------------------------------|-------------------------------|
| Cyber Incident Responder                        | Protection and Defense                               | Киберполигон (учения Red/Blue Team)         | Командные учения по сценарию  |
| Penetration Tester                              | Protection and Defense                               | CTF, платформы типа Hack The Box            | CTF, отчёт о тестировании     |
| Digital Forensics Investigator                  | Investigation                                        | Песочница, анализ образов                   | Кейс с заключением эксперта   |
| Threat Intelligence Specialist                  | Cyberspace Intelligence                              | Кейс-метод, работа с источниками об угрозах | Аналитический отчёт           |
| Cybersecurity Implementer, Architect            | Implementation and Operation; Design and Development | Лабораторные в песочнице, проектная работа  | Защита проекта                |
| Risk Manager, Auditor, Legal/Compliance Officer | Oversight and Governance                             | Деловые игры, кейс-метод                    | Аудит учебной организации     |
| CISO                                            | Oversight and Governance                             | Штабные учения (tabletop)                   | Разбор управленческих решений |

## Обсуждение

Результаты согласуются с выводами обзора [18]: игровые и практические методы прежде всего вовлекают обучающихся, а прирост знаний появляется тогда, когда они сочетаются с систематической теорией и рефлексией. Исходя из этого, предлагается **гибридная модель подготовки**, состоящая из трёх блоков:

- **теоретический блок** строится на адаптивных модулях LMS: они выравнивают уровень обучающихся и позволяют управлять когнитивной нагрузкой [14];
- **практический блок** проходит в песочницах и на киберполигонах, где обучающиеся отрабатывают сценарии под свой целевой профиль (таблица 5);
- **контрольный блок** проводится в формате CTF-соревнований и командных учений, что даёт объективную оценку готовности действовать в условиях реальной атаки.

Практический блок организован по циклу Колба [13] (рисунок 1). Ошибка в изолированной среде ничем не грозит и сама становится материалом для обучения.

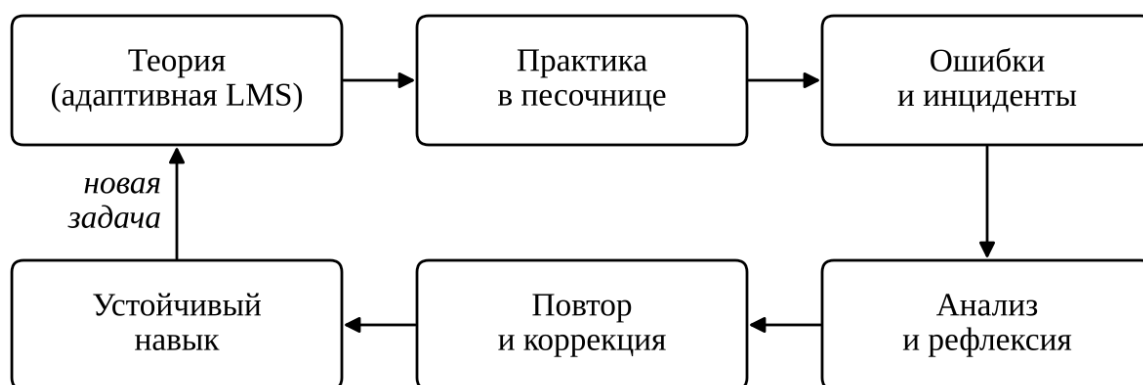


Рисунок 1 – Цикл практико-ориентированного обучения в изолированной среде (разработано авторами на основе [13])

Мотивационно-адаптивный контур модели (рисунок 2) связывает геймификацию с аналитикой успеваемости. Результаты выполненных заданий поступают в адаптивный модуль, и он подбирает следующее задание под уровень конкретного обучающегося. Так поддерживается и потребность в компетентности [16], и оптимальная сложность заданий [14].

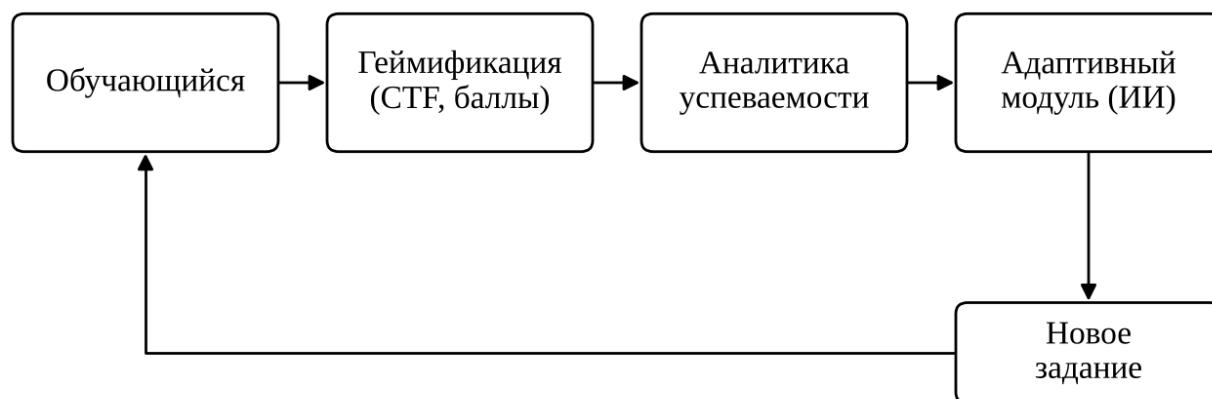


Рисунок 2 – Мотивационно-адаптивный контур гибридной модели (разработано авторами)

**Ограничения исследования.** Исследование носит аналитический характер, и эффективность предложенной модели экспериментально не проверялась. Платформы сравнивались по их открытым описаниям, а соотнесение ролей и методов отражает экспертное мнение авторов. Дальнейшая работа предполагает апробацию модели в учебном процессе на контрольной и экспериментальной группах.

### **Практические рекомендации**

Вузам Казахстана, которые ведут программы по информационной безопасности, можно рекомендовать следующее:

- 1) описывать результаты обучения по образовательной программе через профили ECSF, а задания в отдельных дисциплинах формулировать на основе утверждений TKS из NICE;
- 2) сделать работу в изолированных средах (облачных песочницах, на киберполигонах) обязательной частью технических дисциплин;
- 3) часть привычных тестов заменить CTF-заданиями и командными учениями, оставив письменный разбор решений для развития рефлексии;
- 4) встраивать адаптивные модули в университетские LMS, чтобы выстраивать индивидуальные траектории обучения;
- 5) в подготовке по управленческим и правовым профилям дополнять технические платформы деловыми играми и штабными учениями;
- 6) опираться на национальную статистику инцидентов (ботнеты, фишинг) при разработке учебных сценариев.

### **Заключение**

Анализ показал, что NICE Framework и ECSF друг друга дополняют. ECSF удобна, когда нужно спроектировать образовательную программу и согласовать её с рынком труда, а NICE подходит для детальной проработки заданий и оценочных средств. Обзор литературы подтвердил, что практико-ориентированные и игровые методы повышают вовлечённость, но их влияние на знания зависит от того, сочетаются ли они с теорией и рефлексией.

Научная новизна исследования связана с двумя результатами: матрицей соответствия профилей ролей ECSF и категорий NICE ведущим методам обучения и гибридной моделью подготовки, которая объединяет адаптивный теоретический блок, практику в изолированных средах и геймифицированный контроль. Практическая значимость состоит в том, что результаты можно использовать при обновлении образовательных программ по информационной безопасности в казахстанских вузах. В перспективе планируется проверить модель экспериментально и разработать показатели для оценки её эффективности.

### **Список литературы:**

1. Building a Skilled Cyber Security Workforce in Europe: Insights from France, Germany and Poland / D. Eslava [et al.]. – Paris : OECD Publishing, 2024. – 114 p. – (OECD Skills Studies). – DOI: 10.1787/3673cd60-en.

2. Количество кибератак в Казахстане выросло в два раза [Электронный ресурс] // Капитал.kz. – 2025. – 2 мая. – URL: <https://kapital.kz/tehnology/136625/kolichestvo-kiberatak-v-kazahstane-vyroslo-v-dva-raza.html> (дата обращения: 06.10.2026).

3. Россия под прицелом: 75 % кибератак в СНГ нацелены на одну страну [Электронный ресурс] // SecurityLab.ru. – 2024. – URL: <https://www.securitylab.ru/news/551770.php> (дата обращения: 06.10.2026).

4. Gajjar V. R., Taherdoost H. Cybercrime on a Global Scale: Trends, Policies, and Cybersecurity Strategies // 5th International Conference on Mobile Computing and Sustainable Informatics (ICMCSI). – IEEE, 2024. – P. 668–676.
5. Influence of Digital Technologies on Information Security in the Public Administration System / M. Durman [et al.] // Journal of Theoretical and Applied Information Technology. – 2025. – Vol. 103, No. 2. – P. 400–411.
6. Human Factor, a Critical Weak Point in the Information Security of an Organization's Internet of Things / K. Hughes-Lartey [et al.] // Heliyon. – 2021. – Vol. 7, No. 3. – Art. e06522. – DOI: 10.1016/j.heliyon.2021.e06522.
7. Pahnla S., Siponen M., Mahmood A. Employees' Behavior towards IS Security Policy Compliance // Proceedings of the 40th Annual Hawaii International Conference on System Sciences (HICSS'07). – IEEE, 2007. – P. 156b.
8. Zhamburbayeva S., Ilyassova G. A. The Realization of the “Concept of Digital Transformation, Development of the Information and Communication Technologies and Cybersecurity Industry for 2023–2029” by Implementing Blockchain in the Technologies of the Republic of Kazakhstan and the Problems of Its Legal Regulation // Вестник Карагандинского университета. Серия «Право». – 2024. – Т. 29, № 4. – С. 137–145.
9. Workforce Framework for Cybersecurity (NICE Framework) : NIST Special Publication 800-181 Rev. 1 / R. Petersen [et al.]. – Gaithersburg : NIST, 2020. – DOI: 10.6028/NIST.SP.800-181r1.
10. NICE Framework Latest Updates [Электронный ресурс] // National Institute of Standards and Technology. – URL: <https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/nice-framework-latest-updates> (дата обращения: 06.10.2026).
11. European Cybersecurity Skills Framework (ECSF): Role Profiles [Электронный ресурс] / European Union Agency for Cybersecurity (ENISA). – 2022. – URL: <https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles> (дата обращения: 06.10.2026).
12. European Cybersecurity Skills Framework (ECSF): User Manual [Электронный ресурс] / European Union Agency for Cybersecurity (ENISA). – 2022. – URL: <https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework> (дата обращения: 06.10.2026).
13. Kolb D. A. Experiential Learning: Experience as the Source of Learning and Development. – 2nd ed. – Upper Saddle River : Pearson FT Press, 2014. – 416 p.
14. Sweller J. Cognitive Load Theory // Psychology of Learning and Motivation. – 2011. – Vol. 55. – P. 37–76. – DOI: 10.1016/B978-0-12-387691-1.00002-8.
15. Knowles M. S., Holton E. F., Swanson R. A. The Adult Learner: The Definitive Classic in Adult Education and Human Resource Development. – 8th ed. – London : Routledge, 2014. – DOI: 10.4324/9781315816951.
16. Deci E. L., Ryan R. M. The “What” and “Why” of Goal Pursuits: Human Needs and the Self-Determination of Behavior // Psychological Inquiry. – 2000. – Vol. 11, No. 4. – P. 227–268. – DOI: 10.1207/S15327965PLI1104\_01.
17. Hamari J., Koivisto J., Sarsa H. Does Gamification Work? A Literature Review of Empirical Studies on Gamification // Proceedings of the 47th Hawaii International Conference on System Sciences. – IEEE, 2014. – P. 3025–3034. – DOI: 10.1109/HICSS.2014.377.

18. Pahlavanpour O., Gao S. A Systematic Mapping Study on Gamification within Information Security Awareness Programs // *Heliyon*. – 2024. – Vol. 10, No. 19. – Art. e38474. – DOI: 10.1016/j.heliyon.2024.e38474.
19. Weijsenfeld F. G. J., Sarmah D. K. Gamifying Cybersecurity: A Narrative-Driven Approach to Teaching Steganography // *Computers and Education Open*. – 2025. – Vol. 9. – Art. 100288. – DOI: 10.1016/j.caeo.2025.100288.
20. Mpanza A., Gundu T., Futch L. Gamified Defence: Practical Guidelines for Combating Social Engineering Attacks // *Information Security Education. Empowering People Through Information Security Education : WISE 2025*. – Cham : Springer, 2026. – (IFIP Advances in Information and Communication Technology ; vol. 742).
21. CyberVR: An Interactive Learning Experience in Virtual Reality for Cybersecurity-Related Issues / S. Veneruso [et al.] // *Proceedings of the International Conference on Advanced Visual Interfaces (AVI '20)*. – New York : ACM, 2020.
22. Measuring the Impact of E-Learning Platforms on Information Security Awareness / T. Fertig [et al.] // *Learning and Collaboration Technologies : HCII 2019*. – Cham : Springer, 2019. – (Lecture Notes in Computer Science ; vol. 11591). – P. 26–37. – DOI: 10.1007/978-3-030-21814-0\_3.
23. Hijji M., Alam G. Cybersecurity Awareness and Training (CAT) Framework for Remote Working Employees // *Sensors*. – 2022. – Vol. 22, No. 22. – Art. 8663. – DOI: 10.3390/s22228663.
24. Hentea M., Dhillon H. S., Dhillon M. Towards Changes in Information Security Education // *Journal of Information Technology Education: Research*. – 2006. – Vol. 5. – P. 221–233.
25. Armstrong H., Jayaratna N. Internet Security Management: A Joint Postgraduate Curriculum Design // *Journal of Information Systems Education*. – 2002. – Vol. 13, No. 3. – P. 249–258.

## МАЗМҰНЫ – СОДЕРЖАНИЕ – CONTENT

### ӘЛЕУМЕТТІК-ЭКОНОМИКАЛЫҚ ЖӘНЕ ҚҰҚЫҚ ҒЫЛЫМДАРЫ - СОЦИАЛЬНО-ЭКОНОМИЧЕСКИЕ И ЮРИДИЧЕСКИЕ НАУКИ - SOCIO-ECONOMIC AND LEGAL SCIENCES

|                                                                                                                                                                                                                                                                     |     |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| Төлегенов Тимур Сейфуллаулы<br><b>ДИНАМИКА ТУРИСТСКИХ ПОТОКОВ И ЭФФЕКТИВНОСТЬ ИНФРАСТРУКТУРЫ<br/>ТУРКЕСТАНА: ОТ ЭКСТЕНСИВНОГО РОСТА К СМАРТ-УПРАВЛЕНИЮ</b> .....                                                                                                    | 10  |
| Alexander Gorevoy<br><b>WHICH INEQUALITY STATISTICS SURVIVE AN ADMINISTRATIVE BOUNDARY CHANGE?<br/>EVIDENCE FROM KAZAKHSTAN, 2010–2023</b> .....                                                                                                                    | 14  |
| Rakhimov Djalil<br><b>DOES THE SHIFT TO CASHLESS PAYMENTS GO TOGETHER WITH FASTER GROWTH IN<br/>HOUSEHOLD CREDIT? EVIDENCE FROM THE REGIONS OF KAZAKHSTAN, 2023-2025</b> .....                                                                                      | 26  |
| Kazhgerey Asan<br><b>HOW MANY FOOD BASKETS DOES AN AVERAGE WAGE BUY? WAGES AND FOOD PRICES IN<br/>THE 20 REGIONS OF KAZAKHSTAN, 2024-2026</b> .....                                                                                                                 | 37  |
| Tagimova Alua<br><b>WHO WAS LEFT BEHIND? EDUCATION AND FINANCIAL INCLUSION IN KAZAKHSTAN AND<br/>THREE CENTRAL ASIAN NEIGHBOURS, 2021-2024</b> .....                                                                                                                | 44  |
| Wei Wei, Mynzhanova Gulzhakan, Niyetalina Gaukhar<br><b>DIGITAL–PHYSICAL INTEGRATION AND ECONOMIC PERFORMANCE IN INDUSTRIAL<br/>INTEGRATED ENERGY SYSTEMS: A SCENARIO-BASED ANALYSIS OF SMART GRID<br/>CONTROL, BATTERY ENERGY STORAGE, AND DIGITAL TWINS</b> ..... | 51  |
| Xu Fumin, Wei Wei, Ruziyeva Elvira, Moldabekova A.<br><b>FROM CULTURAL RESOURCES TO GLOBAL CONSUMER VALUE: THE BRIDGE–IMC MODEL<br/>AND THE INTERNATIONALIZATION OF BLACK MYTH: WUKONG UNDER THE BELT AND<br/>ROAD INITIATIVE</b> .....                             | 64  |
| Ibraimkhan Alikhan<br><b>WHICH CRIMES CAN A 14-YEAR-OLD BE TRIED FOR? THE LIST IN ARTICLE 15 OF<br/>KAZAKHSTAN'S CRIMINAL CODE COMPARED WITH 30 OTHER JURISDICTIONS</b> .....                                                                                       | 80  |
| Yerboluly Madi<br><b>DID IMPORTED CARS REALLY GET CHEAPER? CHINESE CARS AND THE AVERAGE<br/>CUSTOMS VALUE OF PASSENGER CARS IMPORTED INTO KAZAKHSTAN, 2015-2025</b> .....                                                                                           | 91  |
| Салимбаев Ербол Аманжолович<br><b>АНАЛИЗ ИНВЕСТИЦИОННОЙ АКТИВНОСТИ КАК ИНДИКАТОР ИЗМЕНЕНИЙ<br/>ПОТЕНЦИАЛЬНОГО СПРОСА НА КОНСАЛТИНГОВЫЕ УСЛУГИ</b> .....                                                                                                             | 99  |
| Rambergenov Ramil<br><b>REGIONAL NEW-FIRM FORMATION IN UZBEKISTAN AFTER THE 2017 REFORMS:<br/>PERSISTENCE IN SCALE, CONVERGENCE IN INTENSITY, AND RECOMPOSITION TOWARD<br/>TRADE</b> .....                                                                          | 107 |
| Abdesh Dinara<br><b>FROM A WOMEN'S LEAD TO A MEN'S LEAD: THE GENDER GAP IN DIGITAL PAYMENTS IN<br/>KAZAKHSTAN AND THREE CENTRAL ASIAN NEIGHBOURS, 2021-2024</b> .....                                                                                               | 116 |
| Amangeldi Aidana<br><b>DID SMALL BUSINESS IN KAZAKHSTAN REALLY SHRINK IN 2026? THE NEW TAX CODE,<br/>REGIONAL TAX RATES AND THE FALL IN THE NUMBER OF INDIVIDUAL ENTREPRENEURS</b> .....                                                                            | 124 |

|                                                                                                                                                |     |
|------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| Cheng Che                                                                                                                                      |     |
| <b>BUILD, BUY, OR PARTNER? ENTRY MODE SELECTION AND RISK GOVERNANCE FOR WIND POWER INVESTMENT IN KAZAKHSTAN</b>                                | 133 |
| Wang Liang                                                                                                                                     |     |
| <b>FROM CAPACITY EXPANSION TO SYSTEM VALUE: COORDINATED DEVELOPMENT OF RENEWABLE ENERGY, GRID FLEXIBILITY AND ENERGY STORAGE IN KAZAKHSTAN</b> | 146 |
| Chen Jun                                                                                                                                       |     |
| <b>CONSTRUCTION-PERIOD CREDIT RISK MANAGEMENT FOR LARGE INFRASTRUCTURE PROJECT FINANCE IN KAZAKHSTAN</b>                                       | 159 |
| Alniyaz Danial                                                                                                                                 |     |
| <b>HOW MUCH FUEL DOES A HYBRID REALLY SAVE? A SAME-MODEL COMPARISON OF HYBRID AND GASOLINE CARS IN US FUEL ECONOMY</b>                         | 173 |

#### **ТЕХНИКАЛЫҚ ҒЫЛЫМДАР - ТЕХНИЧЕСКИЕ НАУКИ - TECHNICAL SCIENCE**

|                                                                                                                                                                           |     |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| Nurmakhan Almira                                                                                                                                                          |     |
| <b>ADVANTAGES OF FIBER OPTIC COMMUNICATION OVER TRADITIONAL COPPER CABLES</b>                                                                                             | 180 |
| Kozhabai Bereke                                                                                                                                                           |     |
| <b>SECURITY CHALLENGES IN IOT-BASED TELECOMMUNICATION NETWORKS</b>                                                                                                        | 188 |
| Azamatuly Yerassyl                                                                                                                                                        |     |
| <b>WHY AI-GENERATED CODE FAILS A BENCHMARK: A FAILURE ANALYSIS OF THREE OPEN LANGUAGE MODELS ON 30 HUMANEVAL+ TASKS</b>                                                   | 197 |
| Nurzhan Sanzhar                                                                                                                                                           |     |
| <b>A FEW SHELLS, A FEW OPERATORS: WHERE LOW EARTH ORBIT IS CROWDED IN AN ALTITUDE-INCLINATION MAP OF 16,620 ACTIVE SATELLITES</b>                                         | 206 |
| Askarbek Nurislam                                                                                                                                                         |     |
| <b>CAN THE WEATHER TELL WHICH DAYS IN ASTANA WILL BE POLLUTED? CLASSIFYING PM2.5 EXCEEDANCE DAYS WITH MACHINE LEARNING AND CHECKING THE DATA AGAINST A GROUND MONITOR</b> | 212 |
| Iliyas Arman                                                                                                                                                              |     |
| <b>SHOOTING ON THE MOVE: HOW MUCH AIM A ROBOT LOSES BY IGNORING ITS OWN VELOCITY, AND WHETHER A VIRTUAL-TARGET CORRECTION RECOVERS IT</b>                                 | 223 |
| Ануар Әлімжан Бахытжанұлы, Сексенбаева Айша Курманбековна                                                                                                                 |     |
| <b>СРАВНИТЕЛЬНЫЙ АНАЛИЗ СТАНДАРТОВ И МЕТОДИК ОБУЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ: NICE FRAMEWORK, ECSF И ПРАКТИКО-ОРИЕНТИРОВАННЫЕ ТЕХНОЛОГИИ</b>                                   | 229 |
| Mukhamedzhan Yerganat                                                                                                                                                     |     |
| <b>GROWTH OF GITHUB DEVELOPER COMMUNITIES IN KAZAKHSTAN, UZBEKISTAN AND KYRGYZSTAN, 2020-2026: EVIDENCE FROM THE GITHUB INNOVATION GRAPH</b>                              | 239 |

#### **ПӘНДЕР АРАЛЫҚ ҒЫЛЫМДАР – МЕЖДИСЦИПЛИНАРНЫЕ НАУКИ – INTERDISCIPLINARY SCIENCES**

|                                                                                                                                 |     |
|---------------------------------------------------------------------------------------------------------------------------------|-----|
| Albiyev Asser                                                                                                                   |     |
| <b>HOW MUCH OF AN ARTICLE COUNT IS HUMAN WORK? DECOMPOSING THE CREATION OF FIVE WIKIPEDIAS, 2010–2025</b>                       | 251 |
| Amangeldy Nurbolat                                                                                                              |     |
| <b>HOW MUCH OF KAZAKHSTAN'S URBAN BUILT STOCK PREDATES ITS SEISMIC CODES, AND WHERE DOES THAT STOCK SIT RELATIVE TO HAZARD?</b> | 261 |

Torekhan Sabrina

|                                                                                                             |            |
|-------------------------------------------------------------------------------------------------------------|------------|
| <b>WHERE ALMATY WALKS ITS OWN WAY: INFORMAL SHORTCUTS IN OPENSTREETMAP AND THE DETOURS THEY AVOID .....</b> | <b>267</b> |
|-------------------------------------------------------------------------------------------------------------|------------|

## **ӘЛЕУМЕТТІК ЖӘНЕ ГУМАНИТАРЛЫҚ ҒЫЛЫМДАР - СОЦИАЛЬНО-ГУМАНИТАРНЫЕ НАУКИ - SOCIAL SCIENCES AND HUMANITIES**

Мұқатаева Айзат Амантайқызы, Стамбекова Жанат Байғазықызы, Слямханова Гүлім Болатқызы, Қызырбек Аяулым Ерболқызы

|                                                                                                              |            |
|--------------------------------------------------------------------------------------------------------------|------------|
| <b>ЖАСАНДЫ ИНТЕЛЛЕКТ ДӘУІРІНДЕГІ ҒЫЛЫМИ ТАНЫМ: ПОППЕР, КУН ЖӘНЕ ЛАКАТОС ИДЕЯЛАРЫ ТҮРҒЫСЫНАН ТАЛДАУ .....</b> | <b>272</b> |
|--------------------------------------------------------------------------------------------------------------|------------|

Мұқатаева Айзат Амантайқызы, Сапарханова Мадина Төлегенқызы, Окенова Аружан Муратхановна, Тұрсынғазыева Ақерке Ерболатқызы

|                                                                               |            |
|-------------------------------------------------------------------------------|------------|
| <b>ШӘКӘРІМ ФИЛОСОФИЯСЫНДАҒЫ ЕРКІНДІК ЖӘНЕ МОРАЛЬДЫҚ ТАҢДАУ МӘСЕЛЕСІ .....</b> | <b>282</b> |
|-------------------------------------------------------------------------------|------------|

Komekova Saida

|                                                                                                                                 |            |
|---------------------------------------------------------------------------------------------------------------------------------|------------|
| <b>DO UNHAPPY REVIEWERS MIX IN MORE RUSSIAN? STAR RATINGS AND KAZAKH-RUSSIAN CODE-SWITCHING IN 175,002 ONLINE REVIEWS .....</b> | <b>291</b> |
|---------------------------------------------------------------------------------------------------------------------------------|------------|

Zhumagali Yerbol

|                                                                                                                                                                       |            |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| <b>DOES A BIGGER MODEL CLOSE THE GAP? KAZAKH-LANGUAGE ACCURACY ON KAZAKHSTAN-SPECIFIC VERSUS UNIVERSAL SCHOOL SUBJECTS IN SMALL OPEN-WEIGHT LANGUAGE MODELS .....</b> | <b>304</b> |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|

Abdrakhmanova Madina

|                                                                                                                           |            |
|---------------------------------------------------------------------------------------------------------------------------|------------|
| <b>DOES A MEDAL BUY ATTENTION? WIKIPEDIA VIEWS OF KAZAKHSTAN'S ATHLETES BEFORE AND AFTER THE PARIS 2024 OLYMPIC .....</b> | <b>308</b> |
|---------------------------------------------------------------------------------------------------------------------------|------------|

## **ПЕДАГОГИКАЛЫҚ ЖӘНЕ ПСИХОЛОГИЯЛЫҚ ҒЫЛЫМДАР – ПЕДАГОГИЧЕСКИЕ И ПСИХОЛОГИЧЕСКИЕ НАУКИ – PEDAGOGICAL AND PSYCHOLOGICAL SCIENCES**

Kaldarbek Mergen

|                                                                                                                        |            |
|------------------------------------------------------------------------------------------------------------------------|------------|
| <b>FAMILY OR SCHOOL? SOCIOECONOMIC COMPOSITION AND MATHEMATICS ACHIEVEMENT IN KAZAKHSTAN, PISA 2022 AND 2025 .....</b> | <b>316</b> |
|------------------------------------------------------------------------------------------------------------------------|------------|

Zhenis Adilzhan

|                                                                                                                                                |            |
|------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| <b>WHICH OLYMPIAD PROBLEMS DO STUDENTS TAKE TO THE BOARD? CHOICES AND DEFENCES IN THE 8TH-GRADE LEAGUE OF KARAGANDY MATHBATTLES 2026 .....</b> | <b>323</b> |
|------------------------------------------------------------------------------------------------------------------------------------------------|------------|

Базарбаева Айнура Бектуровна

|                                                                                                                                           |            |
|-------------------------------------------------------------------------------------------------------------------------------------------|------------|
| <b>ДЕТСКИЙ ФОЛЬКЛОР И ПОДВИЖНЫЕ ИГРЫ КАК ИНСТРУМЕНТЫ ФОРМИРОВАНИЯ ОСНОВ ПРАВОВОЙ КУЛЬТУРЫ У ДЕТЕЙ СТАРШЕГО ДОШКОЛЬНОГО ВОЗРАСТА .....</b> | <b>330</b> |
|-------------------------------------------------------------------------------------------------------------------------------------------|------------|

## **БИОЛОГИЯ ҒЫЛЫМДАР - БИОЛОГИЧЕСКИЕ НАУКИ - BIOLOGICAL SCIENCES**

Bazhenova Diana

|                                                                                                                     |            |
|---------------------------------------------------------------------------------------------------------------------|------------|
| <b>GROWTH DYNAMICS OF STERLET (<i>Acipenser ruthenus</i> L.) REARED IN A RECIRCULATING AQUACULTURE SYSTEM .....</b> | <b>333</b> |
|---------------------------------------------------------------------------------------------------------------------|------------|

## **ТУРИСТИЧЕСКИЕ И СПОРТИВНЫЕ НАУКИ - ТУРИСТІК ЖӘНЕ СПОРТ ҒЫЛЫМДАРЫ - TOURISM AND SPORTS SCIENCES**

Төлеп Жазира Маратқызы

|                                                                                                                        |            |
|------------------------------------------------------------------------------------------------------------------------|------------|
| <b>ГАСТРОНОМИЯЛЫҚ ФЕСТИВАЛЬДЕРДІҢ ТУРИСТІК ДЕСТИНАЦИЯ ТАРТЫМДЫЛЫҒЫН ҚАЛЫПТАСТЫРУДАҒЫ РӨЛІ МЕН ДАМУ ҮРДІСТЕРІ .....</b> | <b>340</b> |
|------------------------------------------------------------------------------------------------------------------------|------------|

**ЕСТЕСТВЕННЫЕ НАУКИ - ЖАРАТЫЛЫСТАНУ ҒЫЛЫМДАРЫ - NATURAL SCIENCES**

Нургельдина Асель Ермаковна, Серикбаева Жанерке Алимжановна

**ШЕКАРАСЫЗ ФИЗИКА: ӘР ЕЛДЕГІ ФИЗИКАЛЫҚ БІЛІМДІ САЛЫСТЫРУ ..... 347**